Department of Information Technology

Y2K INFORMATION TECHNOLOGY DIRECTIVE	**NUMBER**: **1999-10**
SUBJECT: Reporting of technology-related Y2K incidents to DOIT during the Year 2000 event & Rollover Plan	**DATE ISSUED**: December 3, 1999
REFERENCES:	**SUPERSEDES**:

To: Agency Secretaries
Department Directors
Chief Information Officers
Year 2000 Project Managers

From: DEPARTMENT OF INFORMATION TECHNOLOGY

The Event Management Center Communications Center (ECC) will monitor the status of technology-related Year 2000 (Y2K) incidents involving California State entities during the Y2K rollover period, and communicate incident information to key stakeholders, as appropriate. A presentation of the strategy for the ECC was presented at the Chief Information Officers (CIO) meeting on Thursday, December 2, 1999.

This directive communicates the requirements for reporting incident information to the ECC. We have included instructions and templates to facilitate communications and incident reporting activities.

We have also included a Sample Y2K Rollover Checklist and a Sample Y2K Rollover Plan Outline to assist you with your rollover planning activities. If used, the samples should be tailored/augmented to meet your entity's specific needs and requirements. For entities that are implementing a rollover plan, please send a copy of the plan to your Department of Information Technology (DOIT) Y2K Oversight Manager, so they may be referenced if the need arises. If you are not, please respond that you are not.

Incident Reporting
Each State entity must report incidents that are Y2K-related, out of the ordinary, or involve a breach of data or system security.

This Directive addresses reporting of technology issues only. This Directive does not supplant or alter State Government Entities established disaster response procedures and systems, including coordination with the Governor's Office of Emergency Services.

Y2K-related incidents reported to Teale Data Center (TDC), Health and Welfare Data Center (HWDC), Hawkins Data Center (HDC), Franchise Tax Board (FTB), or Department of General Services (DGS) Telecommunications

- If a Y2K-related incident involves a system or process normally reported to TDC, HWDC, HDC, FTB, or DGS Telecommunications, the entity should report to the appropriate data center, or DGS Telecommunications, who will in turn report to the ECC using the **Y2K Incident Reporting Template**. The data centers and DGS Telecommunications will continue to update ECC on the reported incidents until resolved.

Y2K-related incidents NOT reported to TDC, HWDC, HDC, FTB, or DGS Telecommunications

- If a Y2K-related incident involves a system or process normally NOT reported to TDC, HWDC, HDC, FTB, or DGS Telecommunications, the entities must report directly to the ECC using the **Y2K Incident Reporting Template**. A separate report must be completed for each incident. Entities must report ongoing status of incidents to the ECC until resolved.

Incident information must be reported to the ECC, based on the frequency outlined in Table 1, as practical, until the incident is resolved.

Table 1 Status Reporting Frequency

Level	Description	Initial Incident Reporting	Incident Status Reporting Frequency
1	Incidents that impact Mission Critical Processes and present a risk to overall business continuity, or other key stakeholders. Existing contingency plans did not account for this occurrence or was not effective.	Within 1 hour of occurrence	Every 2 hours until resolved
2	Incidents that impact operations, but existing contingency plans allow for a partial resumption of operations.	Within 1 hour of occurrence	Every 2 hours until resolved
3	Incidents that impact operations, but existing contingency plans allow for a full resumption of operations.	Within 2 hours of occurrence	Every 4 hours until resolved
4	Incidents that do not impact operations.	Within 6 hours of occurrence	Only after incident is resolved

ECC Operations

The ECC will operate from December 31, 1999 through March 1, 2000. Specifically, the ECC will be staffed 24 hours per day beginning at 08:00(PST) on Friday, December 31, and continuing to 17:00(PST) on Tuesday, January 4, 2000. Incidents are to be reported as they occur, 24 hours per day, during this period.

The ECC will then operate during normal business hours from January 5, 2000 through March 1, 2000. During this time, Y2K-related incidents are to be reported to the ECC during normal business hours of 08:00 to 17:00(PST) Monday through Friday. Any Y2K-related incident occurring outside of this time period should be communicated using existing entity reporting procedures, and then communicated to the ECC during normal operating hours the following business day. If the incident needing immediate attention from DOIT occurs outside of the ECC normal business hours, contact the ECC Telephone at (916) 464-3688.

State Entities reporting directly to the ECC should use the telephone as the primary mode of communicating initial incident and status information. Although the preferred method of communication is by telephone, completed reporting templates may also be faxed or emailed to the ECC if necessary. In the event of loss of telephone service, the state entities will maintain contact with the ECC through use of email, cellular phone, and hand/courier delivery.

The following information provides details for communicating with the ECC during the planned hours of operations.

ECC Contact Information during the Year 2000 Rollover

Preferred Method of Communication		Contact Information
1	**ECC Telephone**	**(916) 464-3688**
2	**ECC Fax**	**(916) 464-3654**
3	**Cellular Phone**	**(916) 715-5325**
4	**ECC email**	**ecc@emc.ca.gov**
5	**ECC Drop Off Location**	**Guard Station 3101 Gold Camp Dr., Rancho Cordova, CA 95670**

This information is for State entity use only.
Press Inquiries should be directed to OES Press Office at (916) 262-1843

Reporting Mission Critical System Operating Schedule

During the rollover, the ECC will be required to respond to the requests from the Governor, the Legislature, and other stakeholders for overall status information on a state entity, or an agency, or the state as a whole. To facilitate this activity, the DOIT requires each entity to provide a schedule indicating the date and time of the first production run in the Year 2000 for each mission critical system. We have developed a spreadsheet consisting of information derived from Schedule E (Systems Inventory) and instructions to assist you with this effort. This spreadsheet and instructions will be sent via email to all CIOs and Y2K Program Managers by December 3, 1999. Please return the completed spreadsheet by December 10, 1999.

Entities must notify the ECC if a Mission Critical System is not operational for any reason, as scheduled, following the rollover.

Entity Contact Information

In an effort to effectively monitor and report Y2K incidents, the ECC requires contact information from each entity. Please complete the attached Y2K Entity Contact Information Form, and fax to your DOIT Y2K Oversight Manager no later than December 10, 1999.

If you have any questions, please contact your DOIT Y2K Oversight Manager.

JEFFREY R. PELL
Year 2000 Program Director
Department of Information Technology

Attachments: (1) Y2K Incident Reporting Template
(2) Sample Y2K Rollover Checklist
(3) Sample Y2K Rollover Plan Outline
(4) Y2K Entity Contact Information Form

(Please check one) ☐ Initial Incident Report ☐ Incident Status Update

Y2K Incident Reporting Template *(See Instructions)*

Entity Name	**Date/Time Reported**	**Incident Number** *(provided by ECC)*
	_____/_____/_____ _____: mm dd yyyy hh mm AM/PM	

Prepared By	**Incident Contact Name**	**Phone Number**

System Name

System Type *(Please select one)*

☐ Embedded System ☐ Hardware ☐ Application ☐ Security

☐ System Software ☐ Network ☐ Other *(Specify)*

Incident Level *(See Instructions)*

☐ 1 ☐ 2 ☐ 3 ☐ 4

Expected/Actual Resolution Date / Time

_____/_____/_____ _____:
mm dd yyyy hh mm AM/PM

Resolved

☐ Yes

☐ No

System Criticality *(Please select one)*

☐ Mission Critical System

☐ Department Critical System

☐ Non Mission Critical System

☐ Other / Unknown

Incident Impact *(Please check as many as apply)*

☐ Entity Operations ☐ Other State Entities

☐ Other Businesses ☐ Public

☐ Others *(Specify)*

External Help Required

☐ Yes ☐ No

If Yes, Explain *(Attach extra pages if required)*

Description of the Incident *(Attach extra pages if required)*

Description of the Impact *(Attach extra pages if required)*

Decision / Actions / Status *(Attach extra pages if required)*

ECC Phone: (916) 464 3688 **ECC Fax:** (916) 464 3654 **ECC Email:** ecc@emc.ca.gov

Y2K Incident Report Template

Any technology-related Y2K incidents involving a system not reported to the TDC, HWDC, Hawkins Data Center, FTB or DGS Telecom should be reported as soon as they occur, or as practical, directly to the ECC. Entities are required to complete a separate incident report for each incident that is Y2K-related, out of the ordinary, or involves a breach of data or system security. (Incidents reported to data centers will be forwarded to the ECC by the data centers and DGS Telecom.)

Reporting Method

Please complete the incident reports with all required information as outlined in the Y2K Incident Reporting Template. Then telephone the ECC at (916) 464-3688 to report the initial incident or the status of already reported incident. If for any reason, you cannot get through to the ECC via phone, please fax the completed form to (916) 464-3654 or email the completed form to ecc@emc.ca.gov. At the time of reporting an incident, the ECC will assign an *Incident Number* to be given to the person reporting the incident. Please record that number in the space marked Incident Number.

The following is a description of the Y2K Incident Report data fields.

Initial Incident / Status Report	Please check one of the boxes to indicate whether this is an initial incident report or a status update for a previously submitted incident report.
Entity Name	Name of the State Entity reporting the incident or status updates.
Date/Time Reported	The date and time the report was communicated to TDC, HWDC, Hawkins, FTB, DGS Telecom, or directly to the ECC.
Incident Number	If reporting initial incident, an Incident Number will be provided by the ECC, and should be recorded in the space provided. If reporting incident status, please record the Incident Number provided by the ECC at the time of initial incident reporting. This Incident Number will assist the entity and the ECC in ongoing tracking of the incident's status.
Prepared By	The name of the person reporting the incident, or providing the status update.
Incident Contact Name	The name of the key individual the ECC may contact for follow-up on the reported incident.
Phone Number	The phone number of the key individual listed in the Incident Contact Name field.
System Name	Name of system, interface, software, hardware or network affected by the incident.
System Type	Place a check mark in the appropriate box to describe the type of system(s) affected by the incident.
Incident Level	Place a check mark in the appropriate box to indicate the current level of the incident: 1. Incidents that impact Mission Critical Processes and present a risk to overall business continuity, or other key stakeholders. Existing contingency plans did not account for this occurrence or was not effective. 2. Incidents that impact operations, but existing contingency plans allow for a partial resumption of operations. 3. Incidents that impact operations, but existing contingency plans allow for a full resumption of operations. 4. Incidents that do not impact operations. If initially reporting an incident, please select the initial level of the incident. If reporting an incident status, please provide the updated incident level.
Expected/Actual Resolution Date/Time	The time and date the incident is expected to be resolved. If the resolved box is checked, please ensure the date and time reflect when the incident was actually resolved.
Resolved	Place a check mark in this box to indicate whether the incident has been resolved, or remains open.
System Criticality	Place a check mark in the appropriate box to indicate the criticality of the system being reported on.
Incident Impact	Place a check mark in the appropriate box (es) to indicate which is/may be affected by the incident.
External Help Required	Place a check mark in the appropriate field to indicate whether external help is required to resolve the incident. External help is defined as resources that may be available to provide assistance from outside the reporting entity.
If Yes, Explain	If external help is required, provide an explanation of the assistance required in this field.
Description of the Incident	Provide a detailed description of the incident. Please provide as much detail as possible for clear understanding of the issue. If reporting a status update, provide any new information since the time of the last report.
Description of the Impact	Provide a detailed description of the impact as defined in the Incident Impact field. If reporting a status update, provide any new information since the time of the last report.
Decision/Actions/Status	Describe the status of the incident and the actions taken or planned, or decisions made to resolve the incident.

If you have questions about this form prior to the Y2K event, call your DOIT Y2K Oversight Manager. For questions during the Y2K event, call the ECC.

SAMPLE Y2K ROLLOVER CHECKLIST

	Command Center Operations	**Y**	**N**	**NA**
	Designated a command center location			
	Identified executive decision maker for rollover period			
	Developed staffing plan for rollover period			
	Identified who will be onsite/on call for each day of rollover			
	Communicated roles and responsibilities for rollover participants			
	Informed staff of their work schedules during rollover			
	Established call in times and numbers to call for on-call staff			
	Trained staff on rollover/command center procedures			
	Acquired equipment/supplies for command center			
	Printed/stored copies of business continuity/contingency/rollover plans & contact lists			
	Incident Reporting			
	Developed system for logging and tracking incidents			
	Defined modes of communication and reporting channels			
	Communicated incident reporting procedures to staff, business partners and stakeholders			
	Facilities/Infrastructure			
	Identified staff to verify operability of facilities/infrastructure equipment/systems (e.g., security systems, elevators, HVAC systems, power, telecommunications, water/wastewater, etc.) prior to the 1st business day in the year 2000			
	Communicated with building manager/utility suppliers to obtain contact information for problem resolution, if necessary.			
	Business Operations			
	Identified subject matter experts to test/review data to confirm system operability prior to 1st scheduled production run			
	Identified triggers for invoking continuity plans			
	Trained staff on contingency/resumption processes/activities			
	Information Technology			
	Documented and implemented a code freeze policy			
	Identified mission critical systems with short tolerances for outages and readied contingency plans for implementation			
	Identified triggers for invoking contingency plans			
	Defined recovery and restart procedures for systems/applications			
	Identified staff availability during the rollover period to verify operability of computer systems/networks and to coordinate problem resolution, if necessary			
	Prioritized support for systems/applications			
	Developed test scripts to validate data and confirm system operability during rollover			
	Scheduled tests of critical systems to confirm operability			
	Developed procedures for notifying users and key stakeholders, including DOIT, of systems operational status after 1st production run			

	IT Systems Security			
	Assessed system and network security-related issues (e.g., confirmed that passwords/licenses/certificates will not expire during rollover period or at other critical dates)			
	Plan to shut down applications/systems during the rollover period. If yes, have shut-down/restart procedures been developed and tested?			
	Plan to reduce/restrict remote access to networks during the rollover period			
	Protected computers and other electrical equipment with UPS systems or surge protectors			
	Tested UPS systems and batteries			
	Instructed users to power off desktop computers before leaving work at the end of December			
	Instructed users to backup hard drives prior to rollover			
	Developed plans to check the security of computing environment (firewalls, security access, etc.)			
	Installed latest version of antivirus software/definitions			
	Scheduled backups of critical databases/systems prior to rollover			
	External Interfaces			
	Contacted key suppliers/business & data exchange partners to verify current remediation/business continuity status			
	Coordinated rollover activities with suppliers/business and data exchange partners			
	Obtained contact information to coordinate problem resolution, if necessary			
	Communications			
	Developed a plan for communicating within organization			
	Distributed copies of communication plan			
	Distributed copies of business continuity/contingency/rollover plans to management and staff			
	Obtained current employee contact information			
	Identified who will contact employees in case of emergency			
	Identified alternate forms of communication			

Sample Y2K Rollover Plan Outline

Purpose of Plan
Define the goals and objectives of the plan (e.g., explain why the plan is necessary; identify the essential elements/critical factors for a successful plan)

Scope of Plan
Define the boundaries for the operations and functions covered by the plan (e.g., ensure that all critical processes and systems are considered/addressed)

Lifecycle of Plan
Define the start and end dates of the rollover plan (e.g., timeframe that the plan covers, beginning with the first operational action and ending with the last operational action; consider when rollovers for various applications/systems will occur)

Plan Maintenance and Distribution
Identify persons responsible for maintaining the plan and who will receive the plan (or various components of the plan)

Related Plans
Reference or attach as appendices any existing plans that provide authorities or include information needed to implement the rollover plan (e.g., Business Continuity and Contingency Plan, Operation Recovery Plan, State of California Emergency Plan, etc.)

Assumptions
Qualifying statements regarding use of plan (e.g., any understandings/premises on which the plan or any of its elements are based)

Rollover Management Structure
Identify rollover participants (e.g., Chief Information Officer, Y2K Project Manager, CPB Project Manager, IT management and specialists, Business process owners and users, Facilities staff, Communications/Public Information Officers, Human Resources, etc) and define roles and responsibilities. Designate executive decision-maker.

Develop rollover staffing plan to support rollover activities. Communicate roles and responsibilities and train staff on rollover procedures.

Communications Plan
Process/procedures for communicating information during the rollover period. Identify who should receive information/notification of events (e.g., staff, management, suppliers, business/data exchange partners, etc.) and obtain current contact information.

Define modes of communication and reporting channels. Identify who will be responsible for internal communications as well as who will communicate with external stakeholders and media.

Business/System Priorities
Identify the most critical business functions/IT systems and applications and order in which they should be recovered.

Command Center Operations
Implement an incident management system to log and track incidents

Establish rapid response procedures for identifying and responding to incidents. Monitor for events to signal activation of contingency plans.

Command Center Staffing Considerations:

- *Executive Decision-Maker*
- *Y2K Project Manager*
- *CPB Project Manager*
- *Technical Support Staff*
- *Business Unit Subject Matter Experts*
- *Business Services/Facilities Staff*
- *Information Security Officer*
- *Public Information Officer*

Define roles and responsibilities for each command center participant. Train staff on command center processes and procedures.

***Note:** The above staffing considerations are suggestions only; the list should be tailored to meet your entity's specific needs. Make sure you have up-to-date contact information for each employee (e.g., home phone number, pager number, cell phone number).*

Recovery Teams/Tasks/Assembly
Identify recovery teams and tasks to be performed during the recovery process. Identify location where recovery team will assemble to begin assessment/recovery process. Train staff on recovery procedures.

Identify recovery priorities; develop checklists for conducting and subsequently reporting damage assessments.

Equipment/Supplies Checklist
Equipment/supplies required for the rollover/recovery effort (e.g., computer/office equipment, forms and supplies, telecommunications equipment, etc.)

Y2K Entity Contact Information Form *(See Instructions)*

Entity Name	Y2K Operations Center Address		Date Reported
	Y2K Operations Center Phone	Y2K Operations Center Fax	_____/_____/_____ mm dd yyyy

	Name	Phone Number	Alternate Phone Number
Department Director or Equivalent			
	Pager / Cell	**Fax**	**Email**	**Comments**
	Planned Working Hours and Dates During the Rollover Period		

	Name	Title	Primary/Alternate Phone Number
Key Contact Prior to Y2K Event			
	Pager / Cell	**Fax**	**Email**	**Comments**

	Name	Title	Primary/Alternate Phone Number
Alternate Contact Prior to Y2K Event			
	Pager / Cell	**Fax**	**Email**	**Comments**

	Name	Title	Primary/Alternate Phone Number
Key Contact During Y2K Event			
	Pager / Cell	**Fax**	**Email**	**Comments**

	Name	Title	Primary/Alternate Phone Number
Alternate Contact During Y2K Event			
	Pager / Cell	**Fax**	**Email**	**Comments**

Information Security Officer	Name	Phone Number	Alternate Phone Number
	Pager / Cell	**Fax**	**Email**	**Comments**

Y2K Rollover Planned Operation Period	Date Range	Operating Hours

Y2K Entity Contact Information Form

The status of technology-related Y2K incidents involving California State entities will be monitored by the EMC Communications Center (ECC) during the Year 2000 event, and communicated to appropriate key stakeholders. Therefore in an effort to effectively monitor and report Y2K-related incidents, the ECC requires contact information for each entity during the rollover period. Please provide this information no later than December 10, 1999. Please fax the attached form to your DoIT Oversight Manager.

The following is a description of the information requested in the attached form.

Entity Name	Name of the State Entity
Y2K Operations Center Address	Location of the State Entity Y2K Operations Center. If no Operations Center is planned, please give the address where the key contact will be during the rollover period.
Date Reported	Date when Entity Contact Information was reported
Department Director or Equivalent Information	Contact information for the Department's Director or equivalent, including expected work hours during the Y2K event.
Key Contact Prior to Y2K Event Information	Primary contact information for the period prior to the Y2K event
Alternate Contact Prior to Y2K Event Information	Alternate contact information for the period prior to the Y2K event
Key Contact During Y2K Event Information	Primary contact information during the Y2K event. Either the Key or the alternate contact should be available during the entire rollover period starting from December 31, 1999 at 8:00AM through January 4, 2000 at 5:00PM.
Alternate Contact During Y2K Event Information	Alternate contact information during the Y2K event. . Either the Key or the alternate contact should be available during the entire rollover period starting from December 31, 1999 at 8:00AM through January 4, 2000 at 5:00PM.
Information Security Officer Information	Contact information for the Information Security Officer
Y2K Rollover Operations Period	The operating hours of the State Entity's Y2K operating center during and following the Y2K rollover period.